

# EXHIBITS A1-A6 (Part 11 of 13)



Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Step 3 <code>max-metric router-lsa [external-lsa {max-metric-value}] [stub-prefix-lsa] [on-startup {seconds} wait-for-bgp tag] [inter-area-prefix-lsa {max-metric-sumisa}]</code></p> <p><b>Example:</b>  <code>switch(config-router)# max-metric router-lsa on-startup wait-for-bgp</code></p> <p>Configures a device that is running the OSPFv3 protocol to advertise a maximum metric so that other devices do not prefer the device as an intermediate hop in their SPF calculations.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 7-42.</p>	<p><b>max-metric router-lsa (OSPFv3)</b></p> <p>The <code>max-metric router-lsa</code> command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p> <p>The no <code>max-metric router-lsa</code> and default <code>max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p> <p>Platform all  Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre> <p>All parameters can be placed in any order.</p> <p>Parameters</p> <ul style="list-style-type: none"> <li><b>EXTERNAL</b> advertised metric value. Values include: <ul style="list-style-type: none"> <li>&lt;no parameter&gt; Metric is set to the default value of 1.</li> <li><code>external-lsa</code> Configures the router to override the External LSA/NSSA-External metric with the maximum metric value.</li> <li><code>external-lsa &lt;1 to 16777215&gt;</code> The configurable range is from 1 to 0xFFFFF. The default value is 0xFFFF000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.</li> </ul> </li> <li><b>STUB</b> advertised metric type. Values include: <ul style="list-style-type: none"> <li>&lt;no parameter&gt; Metric type is set to the default value of 2.</li> <li><code>include-stub</code> Advertises stub links in router-LSA with the max-metric value (0xFFFF).</li> </ul> </li> <li><b>STARTUP</b> limit scope of LSAs. Values include: <ul style="list-style-type: none"> <li>&lt;no parameter&gt; LSA can be translated</li> <li><code>on-startup</code> Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).</li> <li><code>on-startup wait-for-bgp</code> Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</li> <li><code>on-startup &lt;5 to 86400&gt;</code> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.</li> </ul> <p><code>wait-for-bgp</code> or an <code>on-start</code> time value is not included in no and default commands.</p> </li> <li><b>SUMMARY</b> advertised metric value. Values include: <ul style="list-style-type: none"> <li>&lt;no parameter&gt; Metric is set to the default value of 1.</li> <li><code>summary-lsa</code> Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.</li> <li><code>summary-lsa &lt;1 to 16777215&gt;</code> Metric is set to the specified value.</li> </ul> </li> </ul> <p>Example</p> <ul style="list-style-type: none"> <li>This command shows how to configure OSPFv3 to originate router LSAs with the maximum metric until BGP indicates that it has converged: <pre>switch(config-router-ospf3)#max-metric router-lsa on-startup wait-for-bgp switch(config-router-ospf3)#</pre> </li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1519.</p>	<p>Dkt. 419-10 at PDF p. 355</p>


Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>IS-IS Overview</b></p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p><b>IS-IS Areas</b></p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-2.</p>	<p><b>IS-IS Description</b></p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li>• NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li>• Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> <li>• IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured.</li> <li>• IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node.</li> <li>• LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs.</li> <li>• Hello packets – Hello packets, can establish and maintain neighbor relationships.</li> <li>• Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 356</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>IS-IS Overview</b></p> <p>IS-IS sends a <b>hello packet</b> out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p><b>IS-IS Areas</b></p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level1/Level2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level1/Level2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level1/Level 2 routers in an area, you may want to control which Level1/Level2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level1/Level2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-2.</p>	<p><b>IS-IS Description</b></p> <p>IS-IS sends a <b>hello packet</b> out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li>NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li>Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> <li>IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured.</li> <li>IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node.</li> <li>LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs.</li> <li>Hello packets – Hello packets, can establish and maintain neighbor relationships.</li> <li>Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 357</p>



Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>IS-IS Overview</b></p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the "Configuring the Transient Mode for Hello Padding" section on page 9-21.</p> <p><b>IS-IS Areas</b></p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level1/Level2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level1/Level2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level1/Level 2 routers in an area, you may want to control which Level1/Level2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level1/Level2 router sets the attached bit. For more information, see the "Verifying the IS-IS Configuration" section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-2.</p>	<p><b>IS-IS Description</b></p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li>• NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li>• Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> <li>• IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured.</li> <li>• IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node.</li> <li>• LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs.</li> <li>• Hello packets – Hello packets, can establish and maintain neighbor relationships.</li> <li>• Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 358</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>NET and System ID</b></p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p><b>Designated Intermediate System</b></p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> <b>Note</b> No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-3.</p>	<p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li><b>NET and System ID</b> – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li><b>Designated Intermediate System</b> – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 359</p>
<p><b>NET and System ID</b></p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p><b>Designated Intermediate System</b></p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> <b>Note</b> No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-3.</p>	<p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li><b>NET and System ID</b> – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li><b>Designated Intermediate System</b> – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 359</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>NET and System ID</b></p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p><b>Designated Intermediate System</b></p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> <b>Note</b> No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-3.</p>	<p><b>Terms of IS-IS Routing Protocol</b></p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> <li><b>NET and System ID</b> – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID.</li> <li><b>Designated Intermediate System</b> – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 360</p>
<p><b>Overload Bit</b></p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> <li>The router is in a critical condition.</li> <li>Graceful introduction and removal of the router to/from the network.</li> <li>Other (administrative or traffic engineering) reasons such as waiting for BGP convergence.</li> </ul> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-4.</p>	<ul style="list-style-type: none"> <li><b>Overload Bit</b> – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 360</p>
<p><b>Overload Bit</b></p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> <li>The router is in a critical condition.</li> <li>Graceful introduction and removal of the router to/from the network.</li> <li>Other (administrative or traffic engineering) reasons such as waiting for BGP convergence.</li> </ul> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-4.</p>	<ul style="list-style-type: none"> <li><b>Overload Bit</b> – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 360</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>Overload Bit</b></p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> <li>The router is in a critical condition.</li> <li>Graceful introduction and removal of the router to/from the network.</li> <li>Other (administrative or traffic engineering) reasons such as waiting for BGP convergence.</li> </ul> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-4.</p>	<ul style="list-style-type: none"> <li>Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>	<p>Dkt. 419-10 at PDF p. 361</p>



Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><code>isis hello-multiplier num [level-1   level-2]</code></p> <p><b>Example:</b>  <code>switch(config-if)# isis hello-multiplier 20</code></p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-33.</p>	<p><b>isis hello-multiplier</b></p> <p>The <code>isis hello-multiplier</code> command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The <code>isis hello-multiplier</code> command is used to calculate the hold time announced in hello packets by multiplying this number with the configured <code>isis hello-interval</code>.</p> <p>The <code>no isis hello-multiplier</code> and default <code>isis hello-multiplier</code> commands restore the default hello interval of 3 on the configuration mode interface by removing the <code>isis hello-multiplier</code> command from <i>running-config</i>.</p> <p>Platform           all  Command Mode   Interface-Ethernet Configuration                    Interface-Loopback Configuration                    Interface-Port-channel Configuration                    Interface-VLAN Configuration</p> <p><b>Command Syntax</b></p> <p><code>isis hello-multiplier factor</code>  <code>no isis hello-multiplier</code>  <code>default isis hello-multiplier</code></p> <p><b>Parameters</b></p> <ul style="list-style-type: none"> <li><code>factor</code> hello multiplier. Values range from 3 to 100; default is 3</li> </ul> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>These commands configure a hello multiplier of 4 for VLAN 200.</li> </ul> <pre>switch(config)#interface vlan 200 switch(config-if-Vl200)#isis hello-multiplier 4 switch(config-if-Vl200)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	<p>Dkt. 419-10 at PDF p. 362</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>Step 9 <code>route-reflector-client</code></p> <p>Example:</p> <pre>switch(config-router)#neighbor af# route-reflector-client</pre> <p>Configures the device as a BGP route reflector and configures the neighbor as its client. This command triggers an automatic notification and session reset for the BGP neighbor sessions.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 11-33.</p>	<p>A route reflector is configured to re-advertise routes learned through IBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology. The <code>neighbor route-reflector-client</code> command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. The <code>bgp client-to-client reflection</code> command enables client-to-client reflection.</p> <p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Example</p> <ul style="list-style-type: none"> <li>These commands configure the switch as a route reflector and the neighbor at 101.72.14.5 as one of its clients, and set the cluster ID to 172.22.30.101.</li> </ul> <pre>switch(config-router-bgp)#neighbor 101.72.14.5 route-reflector-client switch(config-router-bgp)#bgp cluster-id 172.22.30.101 switch(config-router-bgp)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>	Dkt. 419-10 at PDF p. 363
<p>Static routes have a default administrative distance of 1. A router prefers a static route to a dynamic route because the router considers a route with a low number to be the shortest. If you want a dynamic route to override a static route, you can specify an administrative distance for the static route. For example, if you have two dynamic routes with an administrative distance of 120, you would specify an administrative distance that is greater than 120 for the static route if you want the dynamic route to override the static route.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 13-2.</p>	<p>Static routes have a default administrative distance of 1. Static routes with a higher administrative distance may be overridden by dynamic routing. For example, a static route with a distance of 200 is overridden by default OSPF intra-area routes (distance of 110). Route maps use tags to filter routes.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1720.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1153; Arista User Manual, v. 4.11.1 (1/11/13), at 914; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>	Dkt. 419-10 at PDF p. 363

## Cisco's Documentation

**clear ip igmp interface statistics**

To clear the IGMP statistics for an interface, use the `clear ip igmp interface statistics` command.

`clear ip igmp interface statistics` [*if-type if-number*]

Syntax Description	<i>if-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>if-number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Defaults None

Command Modes Any command mode

Supported User Roles  
network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to clear IGMP statistics for an interface:

```
switch# clear ip igmp interface statistics ethernet 2/1
switch#
```

Related Commands	Command	Description
	show ip igmp interface	Displays information about IGMP interfaces.

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 6.

## Arista's Documentation

**clear ip igmp statistics**

The `clear ip igmp statistics` command resets IGMP transmission statistic counters for the specified interface.

Platform all  
Command Mode Privileged EXEC

## Command Syntax

`clear ip igmp statistics` [*INTF\_ID*]

## Parameters

- INTF\_ID* interface name. Options include:
  - <no parameter> all interfaces.
  - interface ethernet *e\_num* Ethernet interface specified by *e\_num*.
  - interface loopback *l\_num* Loopback interface specified by *l\_num*.
  - interface management *m\_num* Management interface specified by *m\_num*.
  - interface port-channel *p\_num* Port-channel interface specified by *p\_num*.
  - interface vlan *v\_num* VLAN interface specified by *v\_num*.
  - interface xlan *vx\_num* VXLAN interface specified by *vx\_num*.

## Examples

- This command resets IGMP transmission statistic counters on Ethernet 1 interface.

```
switch#clear ip igmp statistics interface ethernet 1
switch#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1794.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 364

## Cisco's Documentation

**ip igmp snooping last-member-query-interval**

To configure a query interval in which the software removes a group, use the **ip igmp snooping last-member-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

**ip igmp snooping last-member-query-interval** *[interval]*

**no ip igmp snooping last-member-query-interval** *[interval]*

**Syntax Description** *interval* Query interval in seconds. The range is from 1 to 25. The default is 1.

**Defaults** The query interval is 1.

**Command Modes** VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.  
Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

**Supported User Roles** network-admin  
vdc-admin

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

**Usage Guidelines** This command does not require a license.  
See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

**Examples** This example shows how to configure a query interval in which the software removes a group:

```
switch(config)# vlan configuration 10
switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3
switch(config-vlan-config)#
```

This example shows how to reset a query interval to the default:

```
switch(config)# vlan configuration 10
switch(config-vlan-config)# no ip igmp snooping last-member-query-interval
switch(config-vlan-config)#
```

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 86.

## Arista's Documentation

**ip igmp last-member-query-interval**

The **ip igmp last-member-query-interval** command configures the switch's transmission interval for sending group-specific or group-source-specific query messages from the configuration mode interface.

When a switch receives a message from a host that is leaving a group it sends query messages at intervals set by this command. The **ip igmp startup-query-count** specifies the number of messages that are sent before the switch stops forwarding packets to the host.

If the switch does not receive a response after this period, it stops forwarding traffic to the host on behalf of the group, source, or channel.

The **no ip igmp last-member-query-interval** and default **ip igmp last-member-query-interval** commands reset the query interval to the default value of one second by removing the **ip igmp last-member-query-interval** command from *running-config*.

Platform	all
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration

## Command Syntax

```
ip igmp last-member-query-interval period
no ip igmp last-member-query-interval
default ip igmp last-member-query-interval
```

## Parameters

- period* transmission interval (deciseconds) between consecutive group-specific query messages.  
Value range: 10 (one second) to 317440 (8 hours, 49 minutes, 4 seconds). Default is 10 (one second).

## Example

- This command configures the last member query interval of 6 seconds for VLAN interface 4.

```
switch(config)#interface vlan 4
switch(config-if-V14)#ip igmp last-member-query-interval 60
switch(config-if-V14)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1799.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1519; Arista User Manual, v. 4.11.1 (1/11/13), at 1216; Arista User Manual v. 4.10.3 (10/22/12), at 1000; Arista User Manual v. 4.9.3.2 (5/3/12), at 785.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 365



## Cisco's Documentation

**ip igmp snooping startup-query-count**

To configure the number of queries sent at startup, use the `ip igmp snooping startup-query-count` command. To return to the default settings, use the `no` form of this command.

`ip igmp snooping startup-query-count value`

`no ip igmp snooping startup-query-count value`

Syntax Description	<i>value</i> Count value. The range is from 1 to 10.				
Defaults	None				
Command Modes	VLAN configuration (config-vlan)				
Supported User Roles	network-admin vdc-admin				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	NX-OS 5.1(1)	This command was introduced.
Release	Modification				
NX-OS 5.1(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				
Examples	<p>This example shows how to configure the number of queries sent at startup:</p> <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><code>show ip igmp snooping</code></td><td>Displays IGMP snooping information.</td></tr> </table>	Command	Description	<code>show ip igmp snooping</code>	Displays IGMP snooping information.
Command	Description				
<code>show ip igmp snooping</code>	Displays IGMP snooping information.				

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 104.

## Arista's Documentation

**ip igmp snooping querier startup-query-count**

The `ip igmp snooping querier startup-query-count` command configures the global *startup query count* value. The *startup query count* specifies the number of query messages that the querier sends on a VLAN during the *startup query interval* (`ip igmp snooping querier startup-query-interval`).

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The *startup-query-interval* and *startup-query-count* parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs use the global *startup query count* value when they are not assigned a value (`ip igmp snooping vlan querier startup-query-count`). VLAN commands take precedence over the global value. The default global value is specified by the robustness variable (`ip igmp snooping robustness-variable`).

The `no ip igmp snooping querier startup-query-count` and default `ip igmp snooping querier startup-query-count` commands restore the default *startup-query-count* value by removing the corresponding `ip igmp snooping querier startup-query-count` command from *running-config*.

Platform all  
Command Mode Global Configuration

## Command Syntax

`ip igmp snooping querier startup-query-count number`

`no ip igmp snooping querier startup-query-count`

`default ip igmp snooping querier startup-query-count`

## Parameters

- number* global startup query count. Value ranges from 1 to 3.

## Example

- These commands configure the global startup query count value of 2, then displays the status of the snooping querier.

```
switch(config)#ip igmp snooping querier startup-query-count 2
switch(config)#show ip igmp snooping querier status
Global IGMP Querier status
```

```
-----
admin state           : Disabled
source IP address     : 0.0.0.0
query-interval (sec)  : 125.0
max-response-time (sec) : 10.0
querier timeout (sec) : 255.0
last-member-query-interval (sec) : 1.0
last-member-query-count : 2 (robustness)
startup-query-interval (sec) : 31.25 (query-interval/4)
startup-query-count   : 2
```

```
-----
Vlan Admin IP Query Response Querier Operational Ver
State Interval Time Timeout State
-----
1 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
100 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
101 Disabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v2
not tab (conf) #
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/201), at 1813.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 366

## Cisco's Documentation

**ip igmp snooping startup-query-interval**

To configure the query interval at startup, use the **ip igmp snooping startup-query-interval** command. To return to the default settings, use the **no** form of this command.

**ip igmp snooping startup-query-interval** *sec*

**no ip igmp snooping startup-query-interval** *sec*

Syntax Description	<i>sec</i> Interval in seconds. The range is from 1 to 18000.	
Defaults	None	
Command Modes	VLAN configuration (config-vlan)	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	NX-OS 5.1(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the query interval at startup: <pre>switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-interval 4 switch(config-vlan-config)#</pre>	
Related Commands	Command	Description
	show ip igmp snooping	Displays IGMP snooping information.

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 105.

## Arista's Documentation

**ip igmp snooping querier startup-query-interval**

The **ip igmp snooping querier startup-query-interval** command configures the global startup query interval value. The *startup query interval* specifies the period between query messages that the querier sends upon startup.

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The *startup-query-interval* and *startup-query-count* parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs use the global *startup query interval* value when they are not assigned a value (**ip igmp snooping vlan querier startup-query-interval**). VLAN commands take precedence over the global value. The default global value equals the query interval divided by four. (**ip igmp snooping querier query-interval**).

The **no ip igmp snooping querier startup-query-interval** and default **ip igmp snooping querier startup-query-interval** commands restore the default method of specifying the startup query interval by removing the corresponding **ip igmp snooping querier startup-query-interval** command from *running-config*.

Platform all  
Command Mode Global Configuration

## Command Syntax

**ip igmp snooping querier startup-query-interval** *period*  
**no ip igmp snooping querier startup-query-interval**  
**default ip igmp snooping querier startup-query-interval**

## Parameters

- period* startup query interval (seconds). Value ranges from 1 to 3600 (1 hour).

## Example

- This command configures the startup query count of one minute for VLAN interface 4.

```
switch(config)#ip igmp snooping querier startup-query-interval 40
switch(config)#show ip igmp snooping querier status
Global IGMP Querier status
```

```
-----
admin state           : Enabled
source IP address     : 0.0.0.0
query-interval (sec)  : 125.0
max-response-time (sec) : 10.0
querier timeout (sec) : 255.0
last-member-query-interval (sec) : 1.0
last-member-query-count : 2 (robustness)
startup-query-interval (sec) : 40.0
startup-query-count    : 2
```

```
-----
Vlan Admin IP      Query Response Querier Operational Ver
      State          Interval Time      Timeout State
-----
1      Enabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v3
100    Enabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v3
101    Enabled 0.0.0.0 125.0 10.0 255.0 Non-Querier v3
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1813.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 367

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record																																		
<div><div>ip igmp snooping version</div><p>To configure the IGMP version number for VLAN, use the <code>ip igmp snooping version</code> command. To return to the default settings, use the <code>no</code> form of this command.</p><pre>ip igmp snooping version value no ip igmp snooping version value</pre><table><tr><td>Syntax Description</td><td>value</td><td>Version number value. The range is from 2 to 3.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure IGMP version number for VLAN: switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#</td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table></div>	Syntax Description	value	Version number value. The range is from 2 to 3.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure IGMP version number for VLAN: switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier version</div><p>The <code>ip igmp snooping querier version</code> command configures the Internet Group Management Protocol (IGMP) snooping querier version on the configuration mode interfaces. Version 3 is the default IGMP version.</p><p>IGMP is enabled by the <code>ip pim sparse-mode</code> command. The <code>ig igmp snooping querier version</code> command does not affect the IGMP enabled status.</p><p>The <code>no ip igmp snooping querier version</code> and default <code>ip igmp snooping querier version</code> commands restore the configuration mode to IGMP version 3 by removing the <code>ip igmp snooping querier version</code> statement from <i>running-config</i>.</p><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table><p>Command Syntax</p><pre>ip igmp snooping querier version version_number no ip igmp snooping querier version default ip igmp snooping querier version</pre><p>Parameters</p><ul style="list-style-type: none"><li><code>version_number</code> IGMP version number. Value ranges from 1 to 3. Default value is 3.</li></ul><p>Example</p><ul style="list-style-type: none"><li>This command configures IGMP snooping querier version 2. switch(config)#ip igmp snooping querier version 2 switch(config)#</li><li>This command restores the IGMP snooping querier to version 2. switch(config)# no ip igmp snooping querier version switch(config)#</li></ul><p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1815.</p><p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1531.</p></div>	Platform	all	Command Mode	Global Configuration	Dkt. 419-10 at PDF p. 368
Syntax Description	value	Version number value. The range is from 2 to 3.																																		
Defaults	None																																			
Command Modes	VLAN configuration (config-vlan)																																			
SupportedUserRoles	network-admin vdc-admin																																			
Command History	Release	Modification																																		
	5.1(1)	This command was introduced.																																		
Usage Guidelines	This command does not require a license.																																			
Examples	This example shows how to configure IGMP version number for VLAN: switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#																																			
Related Commands	Command	Description																																		
	show ip igmp snooping	Displays IGMP snooping information.																																		
Platform	all																																			
Command Mode	Global Configuration																																			

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 108.

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record																																
<div>Examples</div> <div>This example shows how to display information about IGMP snooping queriers:</div> <div><pre>switch(config)# show ip igmp snooping querier</pre><table><thead><tr><th>Vlan</th><th>IP Address</th><th>Version</th><th>Port</th></tr></thead><tbody><tr><td>1</td><td>172.20.50.11</td><td>v3</td><td>fa2/1</td></tr><tr><td>2</td><td>172.20.40.20</td><td>v2</td><td>Router</td></tr></tbody></table><pre>switch(config)#</pre></div> <div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 50.</div>	Vlan	IP Address	Version	Port	1	172.20.50.11	v3	fa2/1	2	172.20.40.20	v2	Router	<div>Example</div> <div><ul style="list-style-type: none"><li>This command displays the querier IP address, version, and port servicing each VLAN.</li></ul></div> <div><pre>switch&gt;show ip igmp snooping querier</pre><table><thead><tr><th>Vlan</th><th>IP Address</th><th>Version</th><th>Port</th></tr></thead><tbody><tr><td>1</td><td>172.17.0.37</td><td>v2</td><td>Po1</td></tr><tr><td>20</td><td>172.17.20.1</td><td>v2</td><td>Po1</td></tr><tr><td>26</td><td>172.17.26.1</td><td>v2</td><td>Cpu</td></tr><tr><td>2028</td><td>172.17.255.29</td><td>v2</td><td>Po1</td></tr></tbody></table><pre>switch&gt;</pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1860.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1568; Arista User Manual, v. 4.11.1 (1/11/13), at 1263; Arista User Manual v. 4.10.3 (10/22/12), at 1074; Arista User Manual v. 4.9.3.2 (5/3/12), at 831; Arista User Manual v. 4.8.2 (11/18/11), at 637.</div>	Vlan	IP Address	Version	Port	1	172.17.0.37	v2	Po1	20	172.17.20.1	v2	Po1	26	172.17.26.1	v2	Cpu	2028	172.17.255.29	v2	Po1	Dkt. 419-10 at PDF p. 369
Vlan	IP Address	Version	Port																															
1	172.20.50.11	v3	fa2/1																															
2	172.20.40.20	v2	Router																															
Vlan	IP Address	Version	Port																															
1	172.17.0.37	v2	Po1																															
20	172.17.20.1	v2	Po1																															
26	172.17.26.1	v2	Cpu																															
2028	172.17.255.29	v2	Po1																															



Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record																												
<div>aaa group server tacacs+</div> <p>To create a TACACS+ server group and enter TACACS+ server group configuration mode, use the <code>aaa group server tacacs+</code> command. To delete a TACACS+ server group, use the <code>no</code> form of this command.</p> <div>aaa group server tacacs+ group-name</div> <div>no aaa group server tacacs+ group-name</div> <table><tr><td>Syntax Description</td><td>group-name</td><td>TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">Global configuration</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">You must use the feature tacacs+ command before you configure TACACS+. This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2"><p>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</p><div>switch# configure terminal</div><div>switch(config)# aaa group server tacacs+ TacServer</div><div>switch(config-radius)#</div><p>This example shows how to delete a TACACS+ server group:</p><div>switch# configure terminal</div><div>switch(config)# no aaa group server tacacs+ TacServer</div></td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-34.</p>	Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.	Defaults	None		Command Modes	Global configuration		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+. This command does not require a license.		Examples	<p>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</p> <div>switch# configure terminal</div> <div>switch(config)# aaa group server tacacs+ TacServer</div> <div>switch(config-radius)#</div> <p>This example shows how to delete a TACACS+ server group:</p> <div>switch# configure terminal</div> <div>switch(config)# no aaa group server tacacs+ TacServer</div>		<div>aaa group server tacacs+</div> <p>The <code>aaa group server tacacs+</code> command enters server-group-tacacs+ configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.</p> <p>A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a <code>tacacs-server host</code> command.</p> <p>The <code>no aaa group server tacacs+</code> and default <code>aaa group server tacacs+</code> commands delete the specified server group from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <div>aaa group server tacacs+ group_name</div> <div>no aaa group server tacacs+ group_name</div> <div>default aaa group server tacacs+ group_name</div> <p>Parameters</p> <ul style="list-style-type: none"><li><code>group_name</code> name (text string) assigned to the group. Cannot be identical to a name already assigned to a RADIUS server group.</li></ul> <p>Commands Available in server-group-tacacs+ Configuration Mode</p> <ul style="list-style-type: none"><li><code>server (server-group-TACACS+ configuration mode)</code></li></ul> <p>Related Commands</p> <ul style="list-style-type: none"><li><code>aaa group server radius</code></li></ul> <p>Example</p> <ul style="list-style-type: none"><li>This command creates the TACACS+ server group named TAC-GR and enters server group configuration mode for the new group.</li></ul> <div>switch(config)#aaa group server tacacs+ TAC-GR</div> <div>switch(config-sg-tacacs+-TAC-GR)#</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 225.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 169; Arista User Manual, v. 4.11.1 (1/11/13), at 127; Arista User Manual v. 4.10.3 (10/22/12), at 119.</p>	Platform	all	Command Mode	Global Configuration	Dkt. 419-10 at PDF p. 370
Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.																												
Defaults	None																													
Command Modes	Global configuration																													
SupportedUserRoles	network-admin vdc-admin																													
Command History	Release	Modification																												
	4.0(1)	This command was introduced.																												
Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+. This command does not require a license.																													
Examples	<p>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</p> <div>switch# configure terminal</div> <div>switch(config)# aaa group server tacacs+ TacServer</div> <div>switch(config-radius)#</div> <p>This example shows how to delete a TACACS+ server group:</p> <div>switch# configure terminal</div> <div>switch(config)# no aaa group server tacacs+ TacServer</div>																													
Platform	all																													
Command Mode	Global Configuration																													

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record						
<p><b>dot1x pae authenticator</b></p> <p>To create the 802.1X authenticator port access entity (PAE) role for an interface, use the <b>dot1x pae authenticator</b> command. To remove the 802.1X authenticator PAE role, use the <b>no</b> form of this command.</p> <p><b>dot1x pae authenticator</b></p> <p><b>no dot1x pae authenticator</b></p> <hr/> <p><b>Syntax Description</b> This command has no arguments or keywords.</p> <hr/> <p><b>Defaults</b> 802.1X automatically creates the authenticator PAE when you enable the feature on an interface.</p> <hr/> <p><b>Command Modes</b> Interface configuration</p> <hr/> <p><b>Supported User Roles</b> network-admin vdc-admin</p> <hr/> <table border="1"> <thead> <tr> <th>Command History</th><th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td></td><td>4.2(1)</td><td>This command was introduced.</td></tr> </tbody> </table> <hr/> <p><b>Usage Guidelines</b></p> <p>You must use the feature <b>dot1x</b> command before you configure 802.1X.</p> <p>When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.</p> <p>This command does not require a license.</p> <hr/> <p><b>Examples</b></p> <p>This example shows how to create the 802.1X authenticator PAE role on an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# dot1x pae authenticator</pre> <p>This example shows how to remove the 802.1X authenticator PAE role from an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# no dot1x pae authenticator</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-191.</p>	Command History	Release	Modification		4.2(1)	This command was introduced.	<p><b>dot1x pae authenticator</b></p> <p>The <b>dot1x pae authenticator</b> command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</p> <p>The <b>no dot1x pae authenticator</b> and <b>default dot1x pae authenticator</b> commands restore the switch default by deleting the corresponding <b>dot1x pae authenticator</b> command from <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Management Configuration</p> <p><b>Command Syntax</b></p> <p><b>dot1x pae authenticator</b> <b>no dot1x pae authenticator</b> <b>default dot1x pae authenticator</b></p> <p><b>Example</b></p> <ul style="list-style-type: none"> <li>This command configures the port as an IEEE 802.1x port access entity (PAE) authenticator, which enables IEEE 802.1x on the port but does not allow clients connected to the port to be authorized, use the <b>dot1x pae authenticator</b> interface configuration command.</li> </ul> <pre>switch(config-if-Et1)#interface ethernet 2 switch(config-if-Et1)#dot1x pae authenticator switch(config-if-Et1)#</pre> <ul style="list-style-type: none"> <li>This example shows how to disable IEEE 802.1x authentication on the port.</li> </ul> <pre>switch(config-if-Et1)#interface ethernet 2 switch(config-if-Et1)#no dot1x pae authenticator switch(config-if-Et1)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 566.</p>	<p>Dkt. 419-10 at PDF p. 371</p>
Command History	Release	Modification						
	4.2(1)	This command was introduced.						

## Cisco's Documentation

**dot1x timeout quiet-period**

To configure the 802.1X quiet-period timeout globally or for an interface, use the **dot1x timeout quiet-period** command. To revert to the default, use the **no** form of this command.

**dot1x timeout quiet-period** *seconds*

**no dot1x timeout quiet-period**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.
---------------------------	----------------	--

<b>Defaults</b>	Global configuration: 60 seconds Interface configuration: The value of the global configuration
-----------------	--

<b>Command Modes</b>	Global configuration Interface configuration
----------------------	---

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.
-------------------------	---

You must use the **feature dot1x** command before you configure 802.1X.

**Note**

You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

<b>Examples</b>	This example shows how to configure the global 802.1X quiet-period timeout:
-----------------	---

```
switch# configure terminal
switch(config)# dot1x timeout quiet-period 45
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-200.

## Arista's Documentation

**dot1x timeout quiet-period**

The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.

The **no dot1x timeout quiet-period** and **default dot1x timeout quiet-period** commands restore the default advertisement interval of 60 seconds by removing the corresponding **dot1x timeout quiet-period** command from *running-config*.

<b>Platform</b>	all
<b>Command Mode</b>	Interface-Ethernet Configuration Interface-Management Configuration

**Command Syntax**

**dot1x timeout quiet-period** *quiet\_time*

**no dot1x timeout quiet-period**

**default dot1x timeout quiet-period**

**Parameters**

- quiet\_time* advertisement interval (seconds). Values range from 1 to 65535. Default value is 60.

**Example**

- This command sets the number of seconds that an authenticator port waits after a failed authentication with a client before accepting authentication requests again.

```
switch(config)#interface Ethernet 1
switch(config-if-Et1)#dot1x timeout quiet-period 600
switch(config-if-Et1)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 569.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 372

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>To use this command, you must enable the DHCP snooping feature (see the <b>feature dhcp</b> command).</p> <p>You can configure up to four DHCP server IP addresses on Layer 3 Ethernet interfaces and subinterfaces, VLAN interfaces, and Layer 3 port channels. In Cisco NX-OS Release 4.0.2 and earlier releases, you can configure only one DHCP server IP address on an interface.</p> <p>When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP addresses specified on that interface. The relay agent forwards replies from all DHCP servers to the host that sent the request.</p> <p>This command does not require a license.</p> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-309.</p>	<p>The <code>ip dhcp snooping information option</code> command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.</p> <p>DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.</p>	<p>Dkt. 419-10 at PDF p. 373</p>



## Cisco's Documentation

**ip dhcp relay information option**

To enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent, use the **ip dhcp relay information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.

**ip dhcp relay information option**

**no ip dhcp relay information option**

**Syntax Description** This command has no arguments or keywords.

**Defaults** By default, the device does not insert and remove option-82 information on DHCP packets forwarded by the relay agent.

**Command Modes** Global configuration

**Supported User Roles** network-admin  
vdc-admin

Release	Modification
4.0(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command). This command does not require a license.

**Examples** This example shows how to enable the DHCP relay agent to insert and remove option-82 information to and from packets it forwards:

```
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)#
```

Command	Description
<b>ip dhcp relay</b>	Enables or disables the DHCP relay agent.
<b>ip dhcp relay address</b>	Configures the IP address of a DHCP server on an interface.
<b>ip dhcp relay sub-option type cisco</b>	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.
<b>ip dhcp snooping</b>	Globally enables DHCP snooping on the device.

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.

## Arista's Documentation

**ip dhcp relay information option (Global)**

The **ip dhcp relay information option** command configures the switch to attach tags to DHCP requests before forwarding them to the DHCP servers designated by **ip helper-address** commands. The **ip dhcp relay information option circuit-id** command specifies the tag contents for packets forwarded by the interface that it configures.

The **no ip dhcp relay information option** and default **ip dhcp relay information option** commands restore the switch's default setting of not attaching tags to DHCP requests by removing the **ip dhcp relay information option** command from *running-config*.

Platform	all
Command Mode	Global Configuration

**Command Syntax**

**ip dhcp relay information option**  
**no ip dhcp relay information option**  
**default ip dhcp relay information option**

**Related Commands**

These commands implement DHCP relay agent.

- ip helper-address**
- ip dhcp relay always-on**
- ip dhcp relay information option circuit-id**

**Example**

- This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.

```
switch(config)#ip dhcp relay information option
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1264.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 701.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 374

Cisco's Documentation			Arista's Documentation	Supporting Evidence In The Record
Related Commands	Command	Description	Related Commands <ul style="list-style-type: none"><li>ip dhcp snooping globally enables DHCP snooping.</li><li>ip dhcp snooping vlan enables DHCP snooping on specified VLANs.</li><li>ip helper-address enables the DHCP relay agent on a configuration mode interface.</li></ul> Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.	Dkt. 419-10 at PDF p. 375
	ip dhcp relay	Enables or disables the DHCP relay agent.		
	ip dhcp relay address	Configures the IP address of a DHCP server on an interface.		
	ip dhcp relay	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.		
	sub-option type cisco			
	ip dhcp snooping	Globally enables DHCP snooping on the device.		
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.				
Examples	This example shows how to enable VRF support for the DHCP relay agent, which is dependent upon enabling Option-82 support for the DHCP relay agent, and how to configure a DHCP server address on a Layer 3 interface when the DHCP server is in a VRF named SiteA:  switch# configure terminal switch(config)# ip dhcp relay information option switch(config)# ip dhcp relay information option vpn switch(config)# interface ethernet 1/3 switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf SiteA switch(config-if)#		Example <ul style="list-style-type: none"><li>This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.  switch(config)#ip dhcp relay information option switch(config)#</li></ul> Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237.  See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 688.	Dkt. 419-10 at PDF p. 375
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-314.				
Command	Description		Example <ul style="list-style-type: none"><li>This command enables the DHCP relay agent.  switch(config)#ip dhcp relay always-on switch(config)#</li></ul> Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1263.  See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 890; Arista User Manual v. 4.10.3 (10/22/12), at 688.	Dkt. 419-10 at PDF p. 375
feature dhcp	Enables the DHCP snooping feature on the device.			
ip dhcp relay	Enables the DHCP relay agent.			
ip dhcp relay address	Configures an IP address of a DHCP server on an interface.			
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.			
ip dhcp snooping	Globally enables DHCP snooping on the device.			
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-317.				

Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record									
<div><div>ip dhcp smart-relay</div><p>To enable Dynamic Host Configuration Protocol (DHCP) smart relay on a Layer 3 interface, use the <code>ip dhcp smart-relay</code> command. To disable DHCP smart relay on a Layer 3 interface, use the <code>no</code> form of this command.</p><div><div>ip dhcp smart-relay</div><div>no ip dhcp smart-relay</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>Disabled</div></div><div><div>Command Modes</div><div>Interface configuration mode (config-if)</div></div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-319.</p></div> <div><table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>ip dhcp smart-relay</td><td>Enables DHCP smart relay on a Layer 3 interface.</td></tr><tr><td></td><td>ip dhcp relay</td><td>Enable the DHCP relay agent.</td></tr></table><p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-322.</p></div>	Related Commands	Command	Description		ip dhcp smart-relay	Enables DHCP smart relay on a Layer 3 interface.		ip dhcp relay	Enable the DHCP relay agent.	<div><div>ip dhcp smart-relay</div><p>The <code>ip dhcp smart-relay</code> command configures the DHCP smart relay status on the configuration mode interface. DHCP smart relay supports forwarding DHCP requests with a client’s secondary IP addresses in the gateway address field. Enabling DHCP smart relay on an interface requires that DHCP relay is also enabled on that interface.</p><p>By default, an interface assumes the global DHCP smart relay setting as configured by the <code>ip dhcp smart-relay global</code> command. The <code>ip dhcp smart-relay</code> command, when configured, takes precedence over the global smart relay setting.</p><p>The <code>no ip dhcp smart-relay</code> command disables DHCP smart relay on the configuration mode interface. The default <code>ip dhcp smart-relay</code> command restores the interface’s to the default DHCP smart relay setting, as configured by the <code>ip dhcp smart-relay global</code> command, by removing the corresponding <code>ip dhcp smart-relay</code> or <code>no ip dhcp smart-relay</code> statement from <i>running-config</i>.</p><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</div></div><div><div>Command Syntax</div><div><div>ip dhcp smart-relay</div><div>no ip dhcp smart-relay</div><div>default ip dhcp smart-relay</div></div></div><p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1266.</p></div> <div><p>Related Commands</p><ul style="list-style-type: none"><li><code>ip helper-address</code> enables the DHCP relay agent on a configuration mode interface.</li><li><code>ip dhcp smart-relay</code> enables the DHCP smart relay agent on a configuration mode interface.</li></ul><p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1268.</p></div>	<p>Dkt. 419-10 at PDF p. 376</p> <p>Dkt. 419-10 at PDF p. 376</p>
Related Commands	Command	Description									
	ip dhcp smart-relay	Enables DHCP smart relay on a Layer 3 interface.									
	ip dhcp relay	Enable the DHCP relay agent.									

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record												
<div>Examples</div> <div>This example shows how to globally enable DHCP snooping:</div> <div>switch# configure terminal switch(config)# ip dhcp snooping switch(config)#</div> <div>Related Commands</div> <table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>feature dhcp</td><td>Enables the DHCP snooping feature on the device.</td></tr><tr><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr><tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr><tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr></tbody></table> <div>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-323.</div>	Command	Description	feature dhcp	Enables the DHCP snooping feature on the device.	ip dhcp relay	Enables or disables the DHCP relay agent.	ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.	ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.	<div>Command Syntax</div> <div>ip dhcp snooping no ip dhcp snooping default ip dhcp snooping</div> <div>Related Commands</div> <div><ul style="list-style-type: none"><li>ip dhcp snooping information option enables insertion of option-82 snooping data.</li><li>ip dhcp snooping vlan enables DHCP snooping on specified VLANs.</li><li>ip helper-address enables the DHCP relay agent on a configuration mode interface.</li></ul></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.</div>	<div>Dkt. 419-10 at PDF p. 377</div>
Command	Description													
feature dhcp	Enables the DHCP snooping feature on the device.													
ip dhcp relay	Enables or disables the DHCP relay agent.													
ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.													
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.													
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.													



## Cisco's Documentation

**ip dhcp snooping information option**

To enable the insertion and removal of option-82 information for DHCP packets, use the `ip dhcp snooping information option` command. To disable the insertion and removal of option-82 information, use the `no` form of this command.

`ip dhcp snooping information option`

`no ip dhcp snooping information option`

**Syntax Description** This command has no arguments or keywords.

**Defaults** By default, the device does not insert and remove option-82 information.

**Command Modes** Global configuration

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the DHCP snooping feature (see the `feature dhcp` command). This command does not require a license.

**Examples** This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

Related Commands	Command	Description
	<code>ip dhcp relay information option</code>	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
	<code>ip dhcp snooping</code>	Globally enables DHCP snooping on the device.
	<code>ip dhcp snooping trust</code>	Configures an interface as a trusted source of DHCP messages.
	<code>ip dhcp snooping vlan</code>	Enables DHCP snooping on the specified VLANs.

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-325.

## Arista's Documentation

**ip dhcp snooping information option**

The `ip dhcp snooping information option` command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.

DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes.

VLAN snooping on a specified VLAN requires each of these conditions:

- DHCP snooping is globally enabled.
- Insertion of option-82 information in DHCP packets is enabled.
- DHCP snooping is enabled on the specified VLAN.
- DHCP relay is enabled on the corresponding VLAN interface.

When global DHCP snooping is not enabled, the `ip dhcp snooping information option` command persists in *running-config* without any operational effect.

The `no ip dhcp snooping information option` and default `ip dhcp snooping information option` commands disable the insertion of option-82 DHCP snooping information in DHCP packets by removing the `ip dhcp snooping information option` statement from *running-config*.

Platform	Trident
Command Mode	Global Configuration

## Command Syntax

```
ip dhcp snooping information option
no ip dhcp snooping information option
default ip dhcp snooping information option
```

## Related Commands

- `ip dhcp snooping` globally enables DHCP snooping.
- `ip dhcp snooping vlan` enables DHCP snooping on specified VLANs.
- `ip helper-address` enables the DHCP relay agent on a configuration mode interface.

## Example

- These commands enable DHCP snooping on DHCP packets from ports on snooping-enabled VLANs. DHCP snooping was previously enabled on the switch.

```
switch(config)# ip dhcp snooping information option
switch(config)# show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping is operational
DHCP Snooping is configured on following VLANs:
100
DHCP Snooping is operational on following VLANs:
100
Insertion of Option-82 is enabled
Circuit-id format: Interface name:Vlan ID
Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 378

Cisco's Documentation			Arista's Documentation	Supporting Evidence In The Record
Related Commands	Command	Description	<div>ip dhcp snooping vlan</div> <p>The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1271.</p>	Dkt. 419-10 at PDF p. 379
	ip dhcp snooping	Globally enables DHCP snooping on the device.		
	ip dhcp snooping information option	Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.		
	ip dhcp snooping verify mac-address	Enables MAC address verification as part of DHCP snooping.		
	ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.		
	show ip dhcp snooping	Displays general information about DHCP snooping.		
	show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.		
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-328.			
Command	Description	Related Commands <ul style="list-style-type: none"><li>ip dhcp snooping globally enables DHCP snooping.</li><li>ip dhcp snooping vlan enables DHCP snooping on specified VLANs.</li><li>ip dhcp snooping information option enables insertion of option-82 snooping data.</li><li>ip helper-address enables the DHCP relay agent on a configuration mode interface.</li></ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1302.</p>	Dkt. 419-10 at PDF p. 379	
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.			
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.			
show ip dhcp snooping	Displays general information about DHCP snooping.			
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.			
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-330.				

## Cisco's Documentation

**ip dhcp snooping vlan**

To enable DHCP snooping on one or more VLANs, use the `ip dhcp snooping vlan` command. To disable DHCP snooping on one or more VLANs, use the `no` form of this command.

`ip dhcp snooping vlan` *vlan-list*

`no ip dhcp snooping vlan` *vlan-list*

<b>Syntax Description</b>	<i>vlan-list</i>	Range of VLANs on which to enable DHCP snooping. The <i>vlan-list</i> argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.
---------------------------	------------------	--

**Defaults** By default, DHCP snooping is not enabled on any VLAN.

**Command Modes** Global configuration

**Supported User Roles** network-admin  
vdc-admin

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the DHCP snooping feature (see the `feature dhcp` command). This command does not require a license.

**Examples** This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<code>ip dhcp snooping</code>	Globally enables DHCP snooping on the device.
	<code>ip dhcp snooping information option</code>	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
	<code>ip dhcp snooping trust</code>	Configures an interface as a trusted source of DHCP messages.

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-331.

## Arista's Documentation

**ip dhcp snooping vlan**

The `ip dhcp snooping vlan` command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.

VLAN snooping on a specified VLAN requires each of these conditions:

- DHCP snooping is globally enabled.
- Insertion of option-82 information in DHCP packets is enabled.
- DHCP snooping is enabled on the specified VLAN.
- DHCP relay is enabled on the corresponding VLAN interface.

When global DHCP snooping is not enabled, the `ip dhcp snooping vlan` command persists in *running-config* without any operational affect.

The `no ip dhcp snooping information option` and default `ip dhcp snooping information option` commands disable DHCP snooping operability by removing the `ip dhcp snooping information option` statement from *running-config*.

**Platform** Trident  
**Command Mode** Global Configuration

**Command Syntax**

```
ip dhcp snooping vlan v_range
no ip dhcp snooping vlan v_range
default ip dhcp snooping vlan v_range
```

**Parameters**

- *v\_range* VLANs upon which snooping is enabled. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

**Related Commands**

- `ip dhcp snooping` globally enables DHCP snooping.
- `ip dhcp snooping information option` enables insertion of option-82 snooping data.
- `ip helper-address` enables the DHCP relay agent on a configuration mode interface.

**Example**

- These commands enable DHCP snooping globally, DHCP on VLAN interface 100, and DHCP snooping on VLAN 100.

```
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping information option
switch(config)#ip dhcp snooping vlan 100
switch(config)#interface vlan 100
switch(config-if-Vl100)#ip helper-address 10.4.4.4
switch(config-if-Vl100)#show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping is operational
DHCP Snooping is configured on following VLANs:
100
DHCP Snooping is operational on following VLANs:
100
Insertion of Option-82 is enabled
Circuit-id format: Interface name:Vlan ID
Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1302.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 380

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p data-bbox="65 289 898 337"><code>set-dscp-transmit dscp-value</code> Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63.</p> <p data-bbox="58 378 905 440">Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-444.</p>	<p data-bbox="947 297 1066 326"><b>qos dscp</b></p> <p data-bbox="947 350 1801 440">The <code>qos dscp</code> command specifies the default differentiated services code point (DSCP) value of the configuration mode interface. The default DSCP determines the traffic class for non-IP packets that are inbound on DSCP trusted ports. DSCP trusted ports determine the traffic class for inbound packets as follows:</p> <p data-bbox="930 477 1646 506">Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1093.</p> <p data-bbox="930 544 1780 672"><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 991; Arista User Manual, v. 4.11.1 (1/11/13), at 795; Arista User Manual v. 4.10.3 (10/22/12), at 646; Arista User Manual v. 4.9.3.2 (5/3/12), at 576; Arista User Manual v. 4.8.2 (11/18/11), at 666.</p>	<p data-bbox="1850 289 2032 350">Dkt. 419-10 at PDF p. 381</p>



Cisco’s Documentation	Arista’s Documentation	Supporting Evidence In The Record																								
<div><div>policy-map type control-plane</div><p>To create or specify a control plane policy map and enter policy map configuration mode, use the <code>policy-map type control-plane</code> command. To delete a control plane policy map, use the <code>no</code> form of this command.</p><div><div>policy-map type control-plane</div>policy-map-name</div><div><div>no policy-map type control-plane</div>policy-map-name</div></div> <table><tr><td>Syntax Description</td><td>policy-map-name</td><td>Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">Global configuration</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">You can use this command only in the default VDC. This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to specify a control plane policy map and enter policy map configuration mode: <pre>switch# config t switch(config)# policy-map type control-plane PolicyMapA switch(config-pmap)#</pre> This example shows how to delete a control plane policy map: <pre>switch# config t switch(config)# no policy-map type control-plane PolicyMapA</pre></td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-448.</p>	Syntax Description	policy-map-name	Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.	Defaults	None		Command Modes	Global configuration		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	You can use this command only in the default VDC. This command does not require a license.		Examples	This example shows how to specify a control plane policy map and enter policy map configuration mode: <pre>switch# config t switch(config)# policy-map type control-plane PolicyMapA switch(config-pmap)#</pre> This example shows how to delete a control plane policy map: <pre>switch# config t switch(config)# no policy-map type control-plane PolicyMapA</pre>		<div><div>policy-map type control-plane</div><p>The <code>policy-map type control-plane</code> command places the switch in Policy-Map (control plane) configuration mode, which is a group change mode that modifies a control-plane policy map. A policy map is a data structure that consists of class maps that identify a specific data stream and specify bandwidth and shaping parameters that controls its transmission. Control plane policy maps are applied to the control plane to manage traffic.</p><p>The <code>copp-system-policy</code> policy map is supplied with the switch and is always applied to the control plane. <code>Copp-system-policy</code> is the only valid control plane policy map.</p><p>The <code>exit</code> command saves pending policy map changes to <i>running-config</i> and returns the switch to global configuration mode. Policy map changes are also saved by entering a different configuration mode. The <code>abort</code> command discards pending changes, returning the switch to global configuration mode.</p><p>The <code>no policy-map type control-plane</code> and <code>default policy-map type control-plane</code> commands delete the specified policy map by removing the corresponding <code>policy-map type control-plane</code> command and its associated configuration.</p><div><div>Platform</div>FM6000, Petra, Trident</div><div><div>Command Mode</div>Global Configuration</div><p>Command Syntax</p><div><div>policy-map type control-plane</div> copp-system-policy</div><div><div>no policy-map type control-plane</div> copp-system-policy</div><div><div>default policy-map type control-plane</div> copp-system-policy</div><p><code>copp-system-policy</code> is supplied with the switch and is the only valid control plane policy map.</p><p>Commands Available in Policy-Map Configuration Mode</p><ul style="list-style-type: none"><li><code>class (policy-map (control-plane) – FM6000)</code></li><li><code>class (policy-map (control-plane) – Trident)</code></li></ul><p>Related Commands</p><ul style="list-style-type: none"><li><code>class-map type control-plane</code> enters control-plane class-map configuration mode.</li></ul><p>Example</p><ul style="list-style-type: none"><li>This command places the switch in policy-map configuration mode to edit the <code>copp-system-policy</code> policy map.</li></ul><div><div>switch(config)#policy-map type control-plane</div> copp-system-policy</div><div><div>switch(config-pmap-copp-system-policy)#</div></div></div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1194.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 980; Arista User Manual, v. 4.11.1 (1/11/13), at 784.</p>	Dkt. 419-10 at PDF p. 382
Syntax Description	policy-map-name	Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.																								
Defaults	None																									
Command Modes	Global configuration																									
SupportedUserRoles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	You can use this command only in the default VDC. This command does not require a license.																									
Examples	This example shows how to specify a control plane policy map and enter policy map configuration mode: <pre>switch# config t switch(config)# policy-map type control-plane PolicyMapA switch(config-pmap)#</pre> This example shows how to delete a control plane policy map: <pre>switch# config t switch(config)# no policy-map type control-plane PolicyMapA</pre>																									

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p>To view per-entry statistics, use the <code>show access-lists</code> command or the applicable following command:</p> <ul style="list-style-type: none"> <li>• <code>show ip access-lists</code></li> <li>• <code>show ipv6 access-lists</code></li> <li>• <code>show mac access-lists</code></li> </ul> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-517.</p>	<p><b>Displaying Contents of an ACL</b></p> <p>These commands display ACL contents.</p> <ul style="list-style-type: none"> <li>• <code>show ip access-lists</code></li> <li>• <code>show ipv6 access-lists</code></li> <li>• <code>show mac access-lists</code></li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 845.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 724; Arista User Manual, v. 4.11.1 (1/11/13), at 552; Arista User Manual v. 4.10.3 (10/22/12), at 466.</p>	<p>Dkt. 419-10 at PDF p. 383</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>Examples</b></p> <p>This example shows how to display control plane class map information:</p> <pre>switch# show class-map type control-plane</pre> <pre>class-map type control-plane match-any copp-system-class-critical   match access-grp name copp-system-acl-arp   match access-grp name copp-system-acl-msdp  class-map type control-plane match-any copp-system-class-important   match access-grp name copp-system-acl-gre   match access-grp name copp-system-acl-tacas  class-map type control-plane match-any copp-system-class-normal   match access-grp name copp-system-acl-icmp   match redirect dhcp-snoop   match redirect arp-inspect   match exception ip option   match exception ip icmp redirect   match exception ip icmp unreachable</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-552.</p>	<p><b>Example</b></p> <ul style="list-style-type: none"> <li>This command displays all control plane class maps.</li> <li>This command displays the available control plane class maps.</li> </ul> <pre>switch&gt;show class-map type control-plane</pre> <pre>Class-map: CM-CP1 (match-any)   Match: ip access-group name LIST-CP1 Class-map: copp-system-acllog (match-any) Class-map: copp-system-arp (match-any) Class-map: copp-system-arpresolver (match-any) Class-map: copp-system-bpdu (match-any) Class-map: copp-system-glean (match-any) Class-map: copp-system-igmp (match-any) Class-map: copp-system-ipmcmis (match-any) Class-map: copp-system-ipmcrsvd (match-any) Class-map: copp-system-l3destmiss (match-any) Class-map: copp-system-l3slowpath (match-any) Class-map: copp-system-l3ttl1 (match-any) Class-map: copp-system-lacp (match-any) Class-map: copp-system-lldp (match-any) Class-map: copp-system-selfip (match-any) Class-map: copp-system-selfip-tc6to7 (match-any) Class-map: copp-system-sflow (match-any) Class-map: copp-system-tc3to5 (match-any) Class-map: copp-system-tc6to7 (match-any) switch&gt;</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/20140), at 1212.</p>	<p>Dkt. 419-10 at PDF p. 384</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>Examples</b> This example shows how to display the DHCP relay status and configured DHCP server addresses:</p> <pre>switch# show ip dhcp relay DHCP relay service is enabled Insertion of option 82 is enabled Insertion of VPN suboptions is enabled Helper addresses are configured on the following interfaces: Interface          Relay Address    VRF Name ----- Ethernet1/4        10.10.10.1       red switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-630.</p>	<p><b>Example</b></p> <ul style="list-style-type: none"> <li>This command displays the DHCP relay agent configuration status.</li> </ul> <pre>switch&gt;show ip dhcp relay DHCP servers: 172.22.22.11 Vlan1000: DHCP clients are permitted on this interface</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 868; Arista User Manual v. 4.10.3 (10/22/12), at 716.</p>	Dkt. 419-10 at PDF p. 385
<p><b>Examples</b> This example shows how to display general status information about DHCP snooping:</p> <pre>switch# show ip dhcp snooping DHCP snooping service is enabled Switch DHCP snooping is enabled DHCP snooping is configured on the following VLANs: 1,13 DHCP snooping is operational on the following VLANs: 1 Insertion of Option 82 is disabled Verification of MAC address is enabled DHCP snooping trust is configured on the following interfaces: Interface          Trusted ----- Ethernet2/3        Yes switch#</pre> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-634.</p>	<p><b>Example</b></p> <ul style="list-style-type: none"> <li>This command DHCP snooping hardware status.</li> </ul> <pre>switch&gt;show ip dhcp snooping hardware DHCP Snooping is enabled DHCP Snooping is enabled on following VLANs: None Vlans enabled per Slice Slice: FixedSystem None switch&gt;</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1304.</p>	Dkt. 419-10 at PDF p. 385



## Cisco's Documentation

## Examples

This example shows how to use the show port-security command to view the status of the port security feature on a device:

```
switch# show port-security
```

```
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Ethernet1/4	5	1	0	Shutdown

```
switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-661.

## Arista's Documentation

## Example

- These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface.

```
switch(config)#interface ethernet 7
switch(config-if-Et7)#switchport port-security
switch(config-if-Et7)#switchport port-security maximum 2
switch(config-if-Et7)#exit
switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7
switch(config)#mac address-table static 4464.842d.17ce vlan 10 interface ethernet 7
switch(config)#clear mac address-table dynamic interface ethernet 7
switch(config)#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Et7	2	2	0	Shutdown

```
Total Addresses in System: 1
```

```
switch(config)#show port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0034.24c2.8f11	SecureConfigured	Et7	N/A
10	4464.842d.17ce	SecureConfigured	Et7	N/A

```
Total Mac Addresses for this criterion: 2
```

```
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 632.

See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405-06; Arista User Manual v. 4.10.3 (10/22/12), at 336; Arista User Manual v. 4.9.3.2 (5/3/12), at 405-06.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 386

## Cisco's Documentation

## Examples

This example shows how to use the `show port-security address` command to view information about all MAC addresses secured by port security:

```
switch# show port-security address
```

```
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0054.AAB3.770F	STATIC	port-channel1	0
1	00EE.378A.ABCE	STATIC	Ethernet1/4	0

```
switch#
```

This example shows how to use the `show port-security address interface ethernet 1/4` command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security address interface ethernet 1/4
```

Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	00EE.378A.ABCE	STATIC	Ethernet1/4	0

```
switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-664.

## Related Commands

Command	Description
<code>feature dhcp</code>	Enables the DHCP snooping feature on the device.
<code>ip dhcp snooping</code>	Globally enables DHCP snooping on the device.
<code>service dhcp</code>	Enables or disables the DHCP relay agent.
<code>show ip dhcp snooping</code>	Displays general information about DHCP snooping.
<code>show ip dhcp snooping binding</code>	Displays IP-MAC address bindings, including the static IP source entries.

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-695.

## Arista's Documentation

## Example

- This command displays MAC addresses assigned to port-security protected interfaces.

```
switch>show port-security address
```

```
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	164f.29ae.4e14	SecureConfigured	Et7	N/A
10	164f.29ae.4f11	SecureConfigured	Et7	N/A
10	164f.320a.3a11	SecureConfigured	Et7	N/A

```
Total Mac Addresses for this criterion: 3
```

```
switch>
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 698.

See also Arista User Manual v. 4.12.3 (7/17/13), at 562; Arista User Manual, v. 4.11.1 (1/11/13), at 446; Arista User Manual v. 4.10.3 (10/22/12), at 366; Arista User Manual v. 4.9.3.2 (5/3/12), at 338.

## ip dhcp snooping

The `ip dhcp snooping` command enables DHCP snooping globally on the switch. DHCP snooping is a set of layer 2 processes that can be configured on LAN switches and used with DHCP servers to control network access to clients with specific IP/MAC addresses. The switch supports Option-82 insertion, which is a DHCP snooping process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP servers use port information to track host location and IP address usage by authorized physical ports.

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.

## Supporting Evidence In The Record

Dkt. 419-10 at PDF p. 387

Dkt. 419-10 at PDF p. 387

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
<p><b>Usage Guidelines</b> In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software.</p> <p>LLDP must be enabled on the device before you can enable or disable it on any interfaces.</p> <p><b>Note</b> LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM.</p> <p>LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers.</p> <p>Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the switchto vdc command.</p> <p>This command does not require a license.</p> <p>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 174.</p>	<p><b>12.2.4 Guidelines and Limitations</b></p> <p>LLDP has the following configuration guidelines and limitations:</p> <ul style="list-style-type: none"> <li>• LLDP must be enabled on the device before you can enable or disable it on any interface.</li> <li>• LLDP is supported only on physical interfaces.</li> <li>• LLDP can discover up to one device per port.</li> </ul> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.</p>	<p>Dkt. 419-10 at PDF p. 388</p>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record				
<div><div>lldp holdtime</div><div><p>To configure the amount of time that a receiving device should hold the information sent by your device before discarding it, use the lldp holdtime command. To remove the hold time configuration, use the no form of this command.</p><div>lldp holdtimeseconds</div></div><div><div>Syntax Description</div><div>secondsHold time in seconds. The range is from 10 to 255 seconds.</div></div><div><div>Defaults</div><div>120 seconds</div></div><div><div>Command Modes</div><div>Global configuration mode (config)</div></div><div><div>Supported User Roles</div><div>network-admin network-operator vdc-admin vdc-operator</div></div><div><div>Command History</div><div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.0(1)</td><td>This command was introduced.</td></tr></table></div></div><div><div>Usage Guidelines</div><div><p>Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the switchto vdc command.</p><p>This command does not require a license.</p></div></div><div><div>Examples</div><div><p>This example shows how to configure the Link Layer Discovery Protocol (LLDP) hold time:</p><div>switch(config)# lldp holdtime 180 switch(config)#</div><p>This example shows how to remove the LLDP hold time configuration:</p><div>switch(config)# no lldp holdtime 180 switch(config)#</div></div></div><div>Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.</div></div>	Release	Modification	5.0(1)	This command was introduced.	<div><div>lldp holdtime</div><div><p>The lldp holdtime command specifies the amount of time a receiving device should hold the information sent by the device before discarding it.</p><div>Platformall Command ModeGlobal Configuration</div></div><div><div>Command Syntax</div><div>lldp holdtimeperiod no lldp holdtime default lldp holdtime</div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><li>periodThe amount of time a receiving device should hold the LLDPDU information sent before discarding it. Value ranges from 10 to 65535 second; default value is 120 seconds.</li></ul></div></div><div><div>Examples</div><div><ul style="list-style-type: none"><li>This command sets the amount of time to 180 seconds before the receiving device discards the LLDPDU information.<div>switch(config)# lldp holdtime 180 switch(config)#</div></li><li>This command removes the configured time before the receiving device discards the LLDPDU information.<div>switch(config)# no lldp holdtime 180 switch(config)#</div></li></ul></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 585.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 458; Arista User Manual, v. 4.11.1 (1/11/13), at 376.</div></div>	Dkt. 419-10 at PDF p. 389
Release	Modification					
5.0(1)	This command was introduced.					



Cisco's Documentation			Arista's Documentation	Supporting Evidence In The Record
Related Commands	Command	Description	<b>lldp reinit</b>  The lldp reinit command specifies the delay time in seconds for LLDP to initialize on any interface.  Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.  <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 462; Arista User Manual, v. 4.11.1 (1/11/13), at 380.	Dkt. 419-10 at PDF p. 390
	<b>lldp reinit</b>	Specifies the delay time in seconds for LLDP to initialize on any interface.		
Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.				
Related Commands	Command	Description	<b>lldp transmit</b>  The lldp transmit command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.  Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.  <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 446; Arista User Manual, v. 4.11.1 (1/11/13), at 384.	Dkt. 419-10 at PDF p. 390
	<b>lldp transmit</b>	Enables the transmission of LLDP packets on an interface.		
	show lldp interface ethernet	Displays the LLDP configuration on an interface.		
Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 231.				
Related Commands	Command	Description	12.3.3.2 Setting the LLDP Hold Time The lldp holdtime command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it.  Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.  <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.	Dkt. 419-10 at PDF p. 390
	<b>lldp holdtime</b>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.		
Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 232.				